

**National Aeronautics and Space Administration**

**1804.404-70**

**PART 1803—IMPROPER BUSINESS PRACTICES AND PERSONAL CONFLICTS OF INTEREST**

**Subpart 1803.1—Safeguards**

Sec.

1803.104 Procurement integrity.

1803.104-1 Definitions.

**Subpart 1803.70—IG Hotline Posters**

1803.7000 Policy.

1803.7001 Contract clause.

AUTHORITY: 42 U.S.C. 2473(c)(1)

SOURCE: 61 FR 40537, Aug. 5, 1996, unless otherwise noted.

**Subpart 1803.1—Safeguards**

**1803.104 Procurement integrity.**

**1803.104-1 Definitions.**

*Agency ethics official* means for Headquarters, the General Counsel and the Associate General Counsel for General Law, and for each center, the Chief Counsel.

[62 FR 36704, July 9, 1997. Redesignated at 67 FR 30603, May 7, 2002]

**Subpart 1803.70—IG Hotline Posters**

**1803.7000 Policy.**

NASA requires contractors to display NASA hotline posters prepared by the NASA Office of Inspector General on those contracts specified in 1803.7001, so that employees of the contractor having knowledge of waste, fraud, or abuse, can readily identify a means to contact NASA's IG.

[66 FR 29727, June 1, 2001]

**1803.7001 Contract clause.**

Contracting officers must insert the clause at 1852.203-70, Display of Inspector General Hotline Posters, in solicitations and contracts expected to exceed \$5,000,000 and performed at contractor facilities in the United States.

[66 FR 29727, June 1, 2001]

**PART 1804—ADMINISTRATIVE MATTERS**

**Subpart 1804.1—Contract Executive**

Sec.

1804.170 Contract effective date.

**Subpart 1804.4—Safeguarding Classified Information Within Industry**

1804.404-70 Contract clause.

1804.470 Security requirements for unclassified information technology (IT) resources.

1804.470-1 Scope.

1804.470-2 Policy.

1804.470-3 IT Security requirements.

1804.470-4 Contract clause.

AUTHORITY: 42 U.S.C. 2473(c)(1).

SOURCE: 61 FR 40539, Aug. 5, 1996, unless otherwise noted.

**Subpart 1804.1—Contract Execution**

**1804.170 Contract effective date.**

(a) *Contract effective date* means the date agreed upon by the parties for beginning the period of performance under the contract. In no case shall the effective date precede the date on which the contracting officer or designated higher approval authority signs the document.

(b) Costs incurred before the contract effective date are unallowable unless they qualify as precontract costs (see FAR 31.205-32) and the clause prescribed at 1831.205-70 is used.

**Subpart 1804.4—Safeguarding Classified Information Within Industry**

**1804.404-70 Contract clause.**

The contracting officer shall insert the clause at 1852.204-75, Security Classification Requirements, in solicitations and contracts if work is to be performed will require security clearances. This clause may be modified to add instructions for obtaining security clearances and access to security areas that are applicable to the particular acquisition and installation.

**1804.470 Security requirements for unclassified information technology (IT) resources.**

**1804.470–1 Scope.**

This section implements NASA's acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems. Federal policies include the Federal Information System Management Act (FISMA) of 2002, Homeland Security Presidential Directive (HSPD) 12, Clinger-Cohen Act of 1996 (40 U.S.C. 1401 *et seq.*), OMB Circular A-130, Management of Federal Information Resources, and the National Institute of Standards and Technology (NIST) security requirements and standards. These requirements safeguard IT services provided to NASA such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems.

[72 FR 26561, May 10, 2007]

**1804.470–2 Policy.**

NASA IT security policies and procedures for unclassified information and IT are prescribed in NASA Policy Directive (NPD) 2810, Security of Information Technology; NASA Procedural Requirements (NPR) 2810, Security of Information Technology; and interim policy updates in the form of NASA Information Technology Requirements (NITR). IT services must be performed in accordance with these policies and procedures.

[72 FR 26561, May 10, 2007]

**1804.470–3 IT security requirements.**

These IT security requirements cover all NASA contracts in which IT plays a role in the provisioning of services or products (e.g., research and development, engineering, manufacturing, IT outsourcing, human resources, and finance) that support NASA in meeting its institutional and mission objectives. These requirements are applica-

ble where a contractor or subcontractor must obtain physical or electronic (i.e., authentication level 2 and above as defined in NIST Special Publication 800–63, Electronic Authentication Guideline) access to NASA's computer systems, networks, or IT infrastructure. These requirements are also applicable in cases where information categorized as low, moderate, or high by the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, is stored, generated, processed, or exchanged by NASA or on behalf of NASA by a contractor or subcontractor, regardless of whether the information resides on a NASA or a contractor/subcontractor's information system.

[72 FR 26561, May 10, 2007]

**1804.470–4 Contract clause.**

(a) Insert the clause at 1852.204–76, Security Requirements for Unclassified Information Technology Resources, in all solicitations and contracts when contract performance requires contractors to—

(1) Have physical or electronic access to NASA's computer systems, networks, or IT infrastructure; or

(2) Use information systems to generate, store, process, or exchange data with NASA or on behalf of NASA, regardless of whether the data resides on a NASA or a contractor's information system.

(b) Paragraph (d) of the clause allows contracting officers to waive the requirements of paragraphs (b) and (c)(1) through (3) of the clause. Contracting officers must obtain the approval of the—

(1) Center IT Security Manager before granting any waivers to paragraph (b) of the clause; and

(2) The Center Chief of Security before granting any waivers to paragraphs (c)(1) through (3) of the clause.

[72 FR 26561, May 10, 2007]